G.SHDSL Bridge/Router

GRT-101

User's Manual

Copyright

Copyright (C) 2002 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

The is a class B device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Revision

User's Manual for PLANET G.SHDSL Bridge/Router:

Model: GRT-101

Rev: 1.0 (Jul. 2002)

Part No. EM-GRTV1

Table of Contents

TABLE OF CONTENTS....2

CHAPTER 1 OVERVIEW....4

CHAPTER 2 INSTALLATION....7

2.1 FRONT PANEL LEDS....7
2.2 REAR PANEL PORTS....7
2.3 REAR PANEL CONNECTIONS....8
2.4 SETTING UP THE HARDWARE ENVIRONMENT....9

CHAPTER 3 CONFIGURATION....10

3.1 PURPOSE....10
3.2 LOGON PROCEDURE....10
3.2.1 Serial console....10
3.2.2 Telnet....11
3.2.3 Web browser....11
3.3 QUICK INSTALLATION....12
3.3.1 Bridge Mode....12
3.3.2 Routing Mode for PPPoA and PPPoE with IP Sharing....14
3.3.3 Routing Mode for IPoA or EoA....16
3.3.4 LAN-to-LAN Connection with Bridge Mode....18
3.4 OPERATION INTERFACE....20
3.4.1 Multi-level password protection....21
3.5 CONNECTION MODE....22
3.6 BRIDGING MODE....22
3.6.1 Bridge management....22
3.6.2 Static bridge table....23
3.7 ROUTING MODE....24
3.7.1 LAN setting....24
3.7.2 Static routing table....25
3.7.3 NAT/PAT....26
3.7.4 DHCP server....29
3.7.5 DNS proxy....29
3.8 WAN AND ATM VIRTUAL CONNECTION....30
3.8.1 SHDSL operation....30
3.8.2 ATM virtual connection....31
3.8.3 ATM traffic shaping....33

3.8.4 WAN IP address 34
3.8.5 ISP profile for PPP 34
3.9 SYSTEM STATUS AND PERFORMANCE 35
3.10 USER PROFILE 37
3.11 MANAGEMENT SECURITY 38
3.11.1 Telnet port number 38
3.11.2 Legal client IP 39
3.12 SNMP SUPPORT 40
3.12.1 SNMP community 40
3.12.2 SNMP trap 40
3.13 BACKUP AND RESTORE CONFIGURATION 41
3.13.1 Backup configuration 41
3.13.2 Restore configuration 42
3.14 SOFTWARE UPGRADE 43

Chapter 1 Overview

Based on digital subscriber line (DSL) technology, PLANET new DSL product, GRT-101 provides an affordable, flexible, efficient Internet access solution for SOHO customers while reducing deployment and operational costs from service providers. Via sending and receiving user's datagram (often Internet service) over existing telephone lines, GRT-101 concentrates all traffic onto a single high-speed trunk for Internet activities or sharing a corporate intranet. Through the simple-yet-powerful management UI of GRT-101, networks administrators can complete a managed network deployment just in seconds.

SOFTWARE FEATURES

- Easy configuration and management with password control for various application environments
- Efficient IP routing and transparent learning bridge to support broadband Internet services
- Fully ATM protocol stack implementation over SHDSL
- ATM traffic shaping delivers quality-of-service (QoS) guarantees for multimedia applications
- PPP supports user authentication with PAP/CHAP/MS-CHAP
- SNMP management with MIB II
- Getting enhancements and new features via Internet software upgrade

SOFTWARE SPECIFICATIONS

ATM Protocol

ATM adaptation layer type 5 (AAL5)
VC multiplexing and LLC encapsulation
Multi-protocol over AAL5 (RFC 1483/2684 bridged and routed PDU)
Classical IP over ATM (RFC 1577 with MTU = 1500)
Up to 8 PVCs
Traffic shaping CBR/UBR
UNI 3.1/4.0 PVC
I.610 OAM F5 loopback

PPP Support

PPP (RFC 1661)
PPP over AAL5 (RFC 2364)
PPP over Ethernet (RFC 2516)

User authentication with PAP/CHAP/MS-CHAP

Routing Capability

IP routing with static routing and RIPv1/RIPv2
NAT/PAT with virtual server mapping
DHCP server
DNS proxy

Bridging

IEEE 802.1D transparent learning bridge
Up to 128 MAC learning addresses

Configuration

Local console (RS232)
Telnet access
Web-based GUI (HTTP)
Multi-level password protection

Network Management

SNMPv1/SNMPv2 agent
MIB II

Software Upgrading

TFTP download

Hardware Specification

WAN/LAN Ports	RJ-11 SHDSL WAN port x1 10Mbps LAN port x1
Connector	RJ-11 connector for WAN, RJ-45 connector for LAN
Cabling Requirement	G.SHDSL : AWG26 or higher 10 Base T : UTP/STP Category 3 or 5
LEDs	SHDSL , Power Status, WAN Link and Action Status, LAN Link/Active (and 100M Status)
Speed	SHDSL : 192Kbps to 2.304Mbps (64Kbps per channel) LAN Switch : 10 Mbps at half duplex
Power	External power adapter 9V DC, 1000mA

Environmental	Operating temperature: 0° to 45°C
	Storage temperature: -10° to 70°C
Housing	Plastic Case
Dimension	145 mm x 187 mm x 33 mm (L x W x H)

Chapter 2 Installation

2.1 Front Panel LEDs

The LEDs on the front panel indicate the operational status of GRT-101.

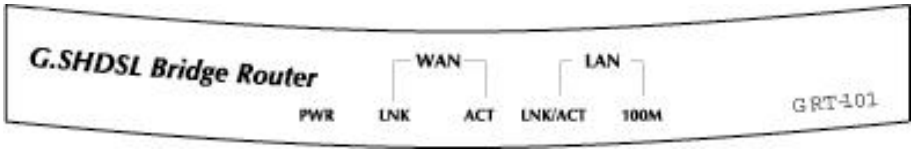


Figure 2-1 Front Panel

The following table describes the LEDs' functions:

Table 2-1 LED Functions

LEDs		Color	Active	Description
PWR		Green	ON	The power adaptor is connected to the Modem
WAN	LNK	Green	ON	SHDSL connection is established
	ACT	Green	ON	Transmit data or receive data over SHDSL link
LAN	LNK/ACT	Green	ON	Transmit data or receive data over Ethernet link
	100M	Green	ON	LED is on 100Mbps mode (reserved for future use)

2.2 Rear Panel Ports

The connectors on the rear panel provide Power, LAN, CONSOLE and LINE interfaces.

Figure 2-2 Rear Panel

The following table describes the connectors' functions:

Table 2-2 Connector Functions

Connectors	Description
DC-IN	Power adaptor inlet: Input voltage 9VDC
LAN	Ethernet 10BaseT for LAN port (RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintained
LINE	SHDSL interface for WAN port (RJ-11)

2.3 Rear Panel Connections

The figure shows the rear panel connections of GRT-101**.**
The STU-R is a standalone and can able to place in desktop. All the external wiring shall be located at the rear panel. The LAN port is a 10 Base-T auto-sensing and half/full duplex configurable Ethernet interface and complied with IEEE 802.3u respectively. The console (RS-232C) interface for configuration are menu-driven operation and can also be configured through Ethernet interface by Telnet or Web-based operation. The power switch operated for power on and power off

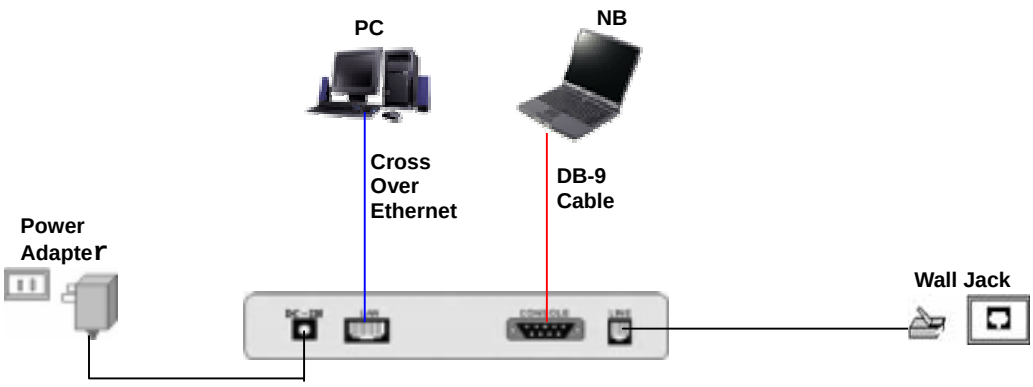


Figure 2-3 Direct Connection with PC or NB

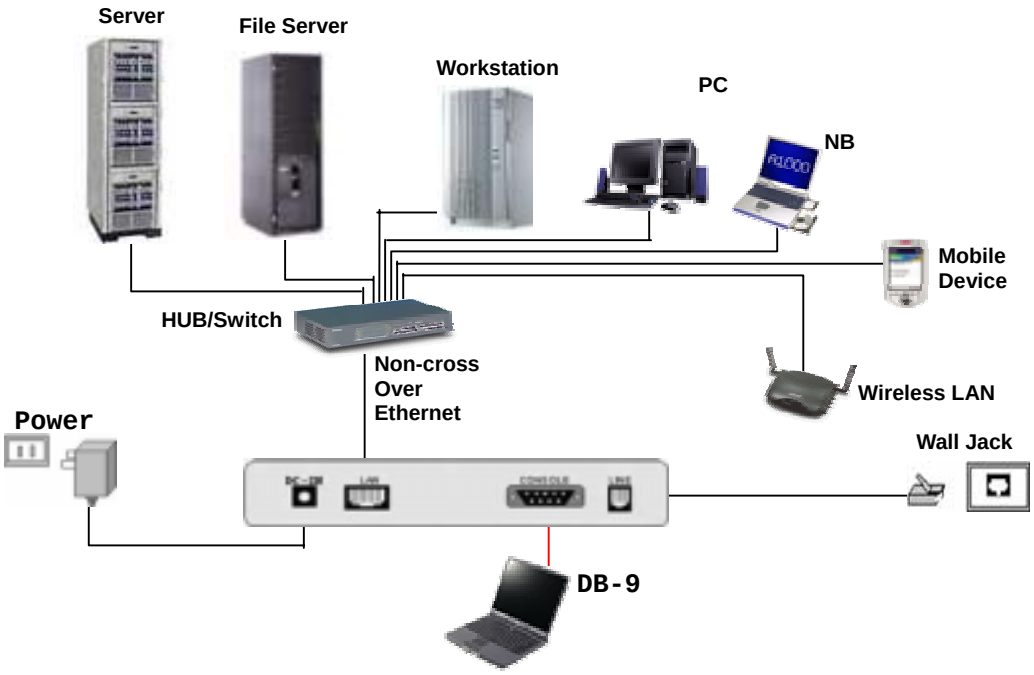


Figure 2-4 Connection with Switch or HUB

2.4 Setting up the hardware environment

Step 1: Connect the power adapter to the port labeled DC-IN on the rear panel of the product.

Step 2: Connect the Ethernet cable.

If GRT is directly connected to PC, the Ethernet cable has to be used cross over one (refer to figure 2-3). If the product is connected to hub or switch, be sure that the hub or switch supporting auto-sensing or not. If yes, both cross over and none cross over Ethernet cable are suitable. If not, only none cross over Ethernet cable could be used (refer to figure 2-4).

Step 3: Connect the phone cable to the product. Connect the other side of phone cable to wall jack.

Step 4: Connect male end of RS-232 cable to the product and female end to any free COM port in PC.

Step 5: Connect the power adapter by plugging power supply.

Chapter 3 Configuration

3.1 Purpose

This chapter provides information about configuring GRT-101.

Note: After you have completed all necessary setting for GRT-101, make sure to write the new configuration to NVRAM by "**write**" command and reboot the system, or all of your changes will not take effect.

3.2 Logon Procedure

There are three methods to logon to GRT-101: serial console, Telnet, and web interface. For the first time configuration, perhaps only the serial console mode could be used because applications requiring Internet protocol (IP) communication, such as Telnet and web interface, are not available unless a management IP is configured properly for your local networking environment. After connecting all the necessary cables described in Chapter 2 Installation, power on GRT-101 and select one of the following procedures to access GRT-101.

Note: It is recommended that only one configuration application is used to setup GRT-101 at any given time, that is, Telnet, serial console and the web management interfaces should not be used simultaneously.

3.2.1 Serial console

Check the connectivity of the RS-232 cable from your computer to the serial port of GRT-101. Start your terminal access program with VT100 terminal emulation. Configure the serial link with baudrate of 9600, 8 data bits, no parity check, 1 stop bit, and no flow-control, and press the SPACE key until the login screen appears. When you see the login screen, you can logon to GRT-101.

```
User: admin
Password: *****
```

Note: If you have not set any user profile for GRT-101, enter the factory default user "**admin**". When the system prompts you for a password, type "**admin**" to enter GRT-101.

After you logon to GRT-101 and before proceeding any further, check the software version of GRT-101 by the command:

```
admin> show system
```

If GRT-101 is out of date, get the latest version from your service provider. See the TFTP command in the section 3.14 Software Upgrade for more information on how to update GRT-101 firmware.

3.2.2 Telnet

Make sure the correct Ethernet cable is used for connecting the LAN port of your computer to GRT-101. The LAN LNK indicator on the front panel shall light if a correct cable is used. Starting your Telnet client with VT100 terminal emulation and connecting to the management IP of GRT-101, wait for the login screen appears. When you see the login screen, you can logon to GRT-101.

```
User: admin
Password: *****
```

Note: The factory default management IP and subnet mask are of 192.168.0.1 and 255.255.255.0, respectively. To change these setting, see section 3.6.1 Bridge management and 3.7.1 LAN setting for routing mode operation. If you have not set any user profile for GRT-101, enter the factory default user "**admin**". When the system prompts you for a password, type "**admin**" to enter GRT-101. For more security issues for remote management interfaces such as Telnet and web interface, see section 3.11 Management Security.

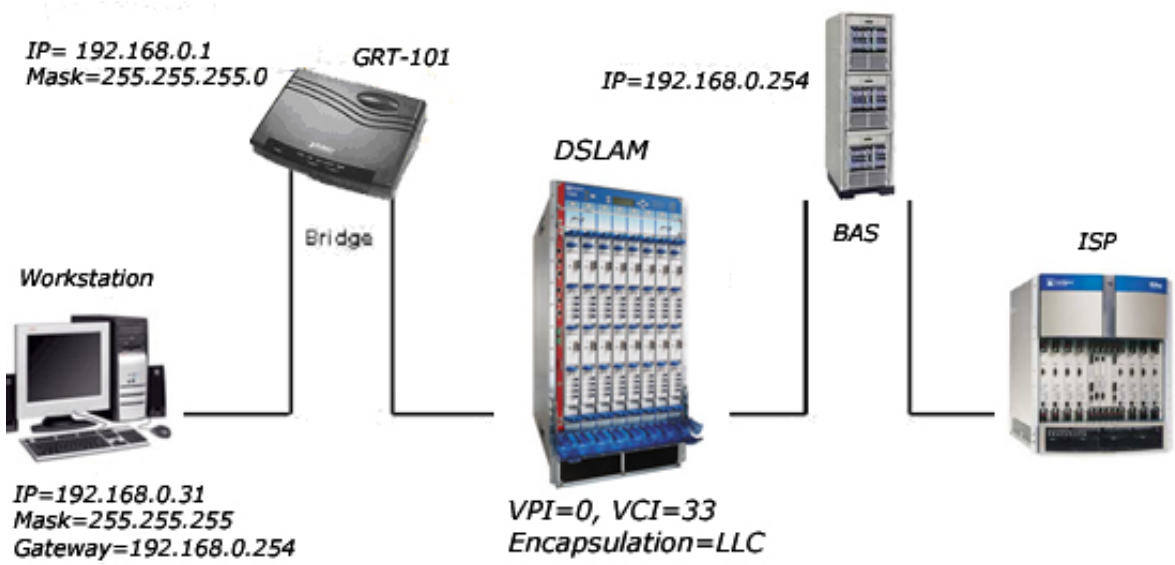
3.2.3 Web browser

Make sure the correct Ethernet cable is used for connecting the LAN port of your computer to GRT-101. The LAN LNK indicator on the front panel shall light if a correct cable is used. Starting your web browser and connecting to the management IP of GRT-101, wait for the login screen appears. When you see the login screen, you can logon to GRT-101.

Note: The factory default management IP and subnet mask are 192.168.0.1 and 255.255.255.0 respectively. To change these setting, see section 3.6.1 Bridge management and 3.7.1 LAN setting. If you have not change password setting for web interface, enter the factory default user "**root**". When GRT prompts you for a password, type "**root**". More security issues for remote management interfaces, please refer to section 3.11 Management Security.

3.3 Quick Installation

3.3.1 Bridge Mode



Web UI Configuration

After connection via web browser,

click Bridge to setup Bridging mode of the

Router and then click Next for the next setting.

Enter WAN1 VPI: 0 and VCI: 33.
Select WAN1 AAL5 Encap: LLC
Enter LAN IP: 192.168.0.1
Enter LAN Sub-net Mask: 255.255.255.0
Enter Gateway: 192.168.0.254 The Gateway is directly pointed to the BAS IP.
Click Next

Click OK to write the new configuration data to the flash memory of GRT-101.

Note: You have to do that otherwise the new configuration parameters will not affect GRT-101.

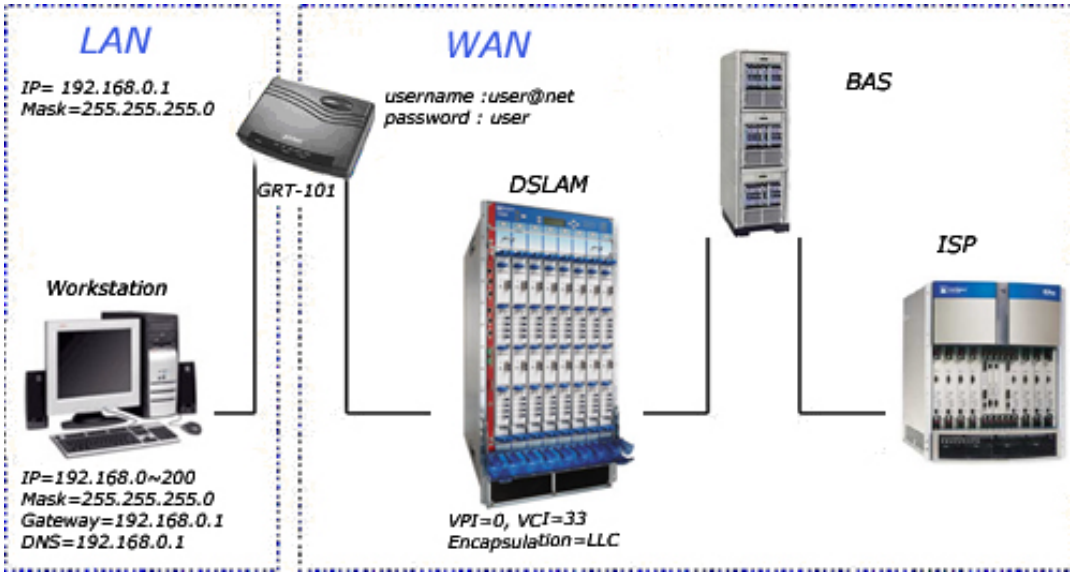
Click Restart GRT-101 will reboot with the new setting.

Console Configuration

Do the following steps:

1 User : admin ↵ password: admin ↵
2 enable ↵ supervisor password: root ↵
3 setup ↵ mode ↵ *Bridge* ↵
4 wan ↵ Interface number (1~8) : 1 ↵
Protocol ↵ : *Ethernet* ↵
vpi_vci : 0 ↵
33 ↵
encap : *LLC* ↵
5 bridge ↵ gateway ↵ 192.168.0.254 ↵
6 lan↵address↵ 192.168.0.1 ↵
255.255.255.0↵
7 (back to root) write ↵ y ↵
y ↵(reboot)

3.3.2 Routing Mode for PPPoA and PPPoE with IP Sharing



Web UI Configuration

For Route Mode with Point-to-Point Protocol over ATM and Ethernet, follow the following setting. First select ROUTE and then click Next for setting others parameters.

Enter VPI: 0 and VCI: 33
Select: LLC
Select: PPP over ATM or PPPoE
Click Next for ISP, LAN and DHCP server setting.

Enter user name provided by ISP: user@net
Enter Password provided by ISP:user
Re-enter Password for confirmation: user
Enter LAN IP Address: 192.168.0.1
Enter Subnet Mask: 255.255.255.0
Select DHCP Service: Enable
Select Next for Dynamic Host Configuration Protocol, DHCP, setting. For DHCP service disable.

Enter Default Gateway: 192.168.0.1 The Gateway is pointed to the LAN IP of GRT-101.
Enter Subnet Mask: 255.255.255.0
Enter DHCP Client Start IP: 192.168.0.2
Enter DHCP Client End IP: 192.168.0.200
Enter Name Server: 192.168.0.1
The DNS server is embedded in GRT-101.
Click Next to write the new setting.

Click OK to write the new configuration data to the flash memory.

Note: You have to do that otherwise the new configuration parameters will not affect GRT-101.

Click Restart to reboot GRT-101.
GRT-101 will reboot with the new setting.

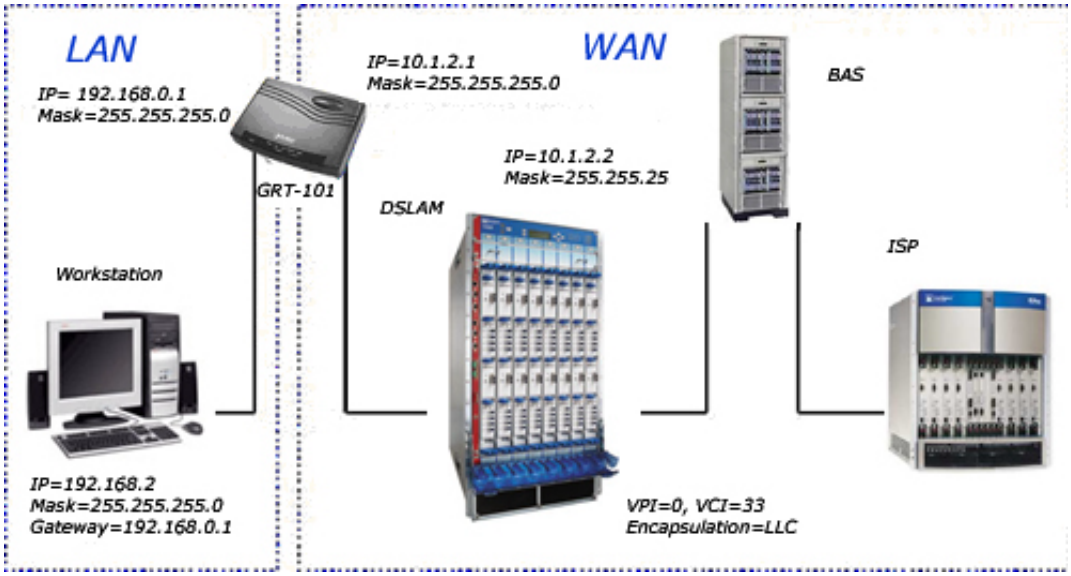
After rebooting, GRT-101 will work with the new configuration.

Console Configuration

Do the following steps:

1. User : admin ↵ password: admin ↵
2. enable ↵ supervisor password: root ↵
3. setup ↵ mode ↵ *Route* ↵
4. wan ↵ Interface number (1~8) : 1 ↵
   protocol ↵ *PPPoA* or *PPPoE* ↵
   vpi_vci ↵ 0 ↵
   33 ↵
   encap ↵ *LLC* ↵
   isp ↵account: user@net ↵
   password: user ↵
   idle time out: 0 ~ 300 ↵ (the unit is in minute)
5. lan ↵ address ↵ 192.168.0.1 ↵
   255.255.255.0 ↵
   attrib ↵ *Virtual* ↵
6. (back to root) write ↵ y ↵
   y ↵(reboot)

3.3.3 Routing Mode for IPoA or EoA

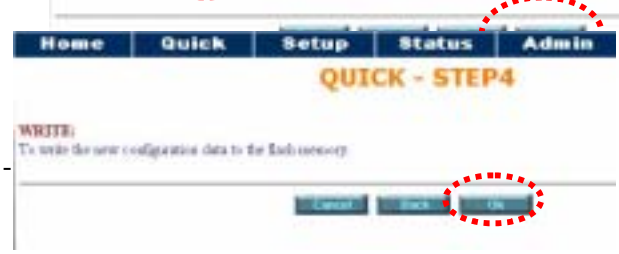


Web UI Configuration

For Route Mode with Classical IP over ATM and Ethernet over ATM, follow the following setting. First select ROUTE and then click Next for setting others parameters.

Enter VPI: 0 and VCI: 33
Select: IP over ATM or Ethernet over ATM
Click Next

Enter WAN1 IP: 10.1.2.1
Enter WAN1 Subnet Mask: 255.255.255.0
Enter LAN IP: 192.168.0.1
Enter LAN Subnet Mask:255.255.255.0
Enter Default Route Gateway: 10.1.2.2
For DHCP enable setting, refer to DHCP setting of Routing Mode with PPPoA or PPPoE with IP Sharing .
Click Next



Click OK to write the new configuration data to the flash memory.

Note: You have to do that otherwise the new configuration parameters will not affect GRT-101.

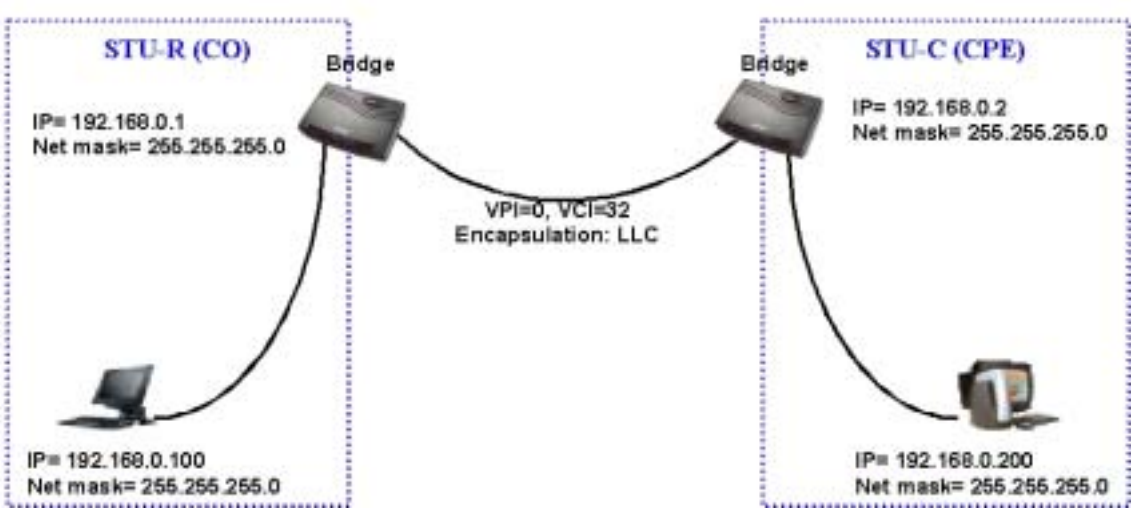
Click Restart to reboot GRT-101. GRT-101 will reboot with the new setting.

Console Configuration

Do the following settings:

1. User : admin ↵ password: admin ↵
2. enable ↵ supervisor password: root ↵
3. setup ↵ mode ↵ *Route* ↵
4. wan ↵ Interface number (1~8) : 1 ↵
   protocol ↵ *IPoA* or *EoA* ↵
   address ↵ 10.1.2.1 ↵
   255.255.255.0 ↵
   vpi_vci ↵ 0 ↵
   33 ↵
   encap ↵ *LLC* ↵
5. lan ↵ address ↵ 192.168.0.1 ↵
   255.255.255.0 ↵
   attrib ↵ *virtual* ↵
6. route ↵ static ↵ add ↵
   IP address: 0.0.0.0
   Subnet mask: 0.0.0.0
   Gateway: 10.1.2.2
7. (back to root) write ↵ y ↵
   y ↵(reboot)

3.3.4 LAN-to-LAN Connection with Bridge Mode



Web UI Configuration

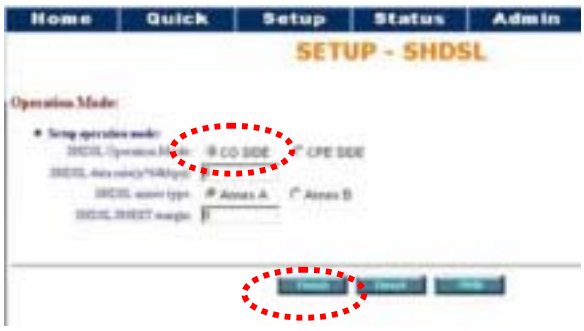
STU-R (CO) side

Click setup to setup the bridge as CO.
Follow the instruction.

Click SHDSL in left side scroll bar to setup the SHDSL operation mode.

Click CO SIDE for setting the bridge as CO.
Click Finish for saving the setting.

Setup the CO Router in bridge mode. The gateway of CO Router is pointed to LAN IP, 192.168.0.2, of CPE Router.



STU-C (CPE) side

Follow the above instruction. The only difference in this configuration is that users have to choose CPE SIDE instead of CO SIDE.

Setup the CPE Router in bridge mode. The gateway of CPE Router is pointed to LAN IP, 192.168.0.1, of CO Router.

Console Configuration

Do the following steps in STU-R side:

1. User : admin ↵ password: admin ↵
2. enable ↵ supervisor password: root ↵
3. setup ↵ mode ↵ *Bridge* ↵

shdsl ↵ *STU-R* ↵

4. wan ↵ Interface number (1~8) : 1 ↵
   Protocol ↵ : *Ethernet* ↵
   vpi_vci : 0 ↵
   33 ↵
   encap : *LLC* ↵
5. lan↵address↵ 192.168.0.1↵
   255.255.255.0↵
6. (back to root) write ↵ y ↵
   y ↵(reboot)

Do the following steps in STU-C side:

1. User : admin ↵ password: admin ↵
2. enable ↵ supervisor password: root ↵
3. setup ↵ mode ↵ *Bridge* ↵

shdsl ↵ *STU-C* ↵

4. wan ↵ Interface number (1~8) : 1 ↵
   Protocol ↵ : *Ethernet* ↵
   vpi_vci : 0 ↵
   33 ↵
   encap : *LLC* ↵
5. lan↵address↵ 192.168.0.2 ↵
   255.255.255.0↵
6. (back to root) write ↵ y ↵
   y ↵(reboot)

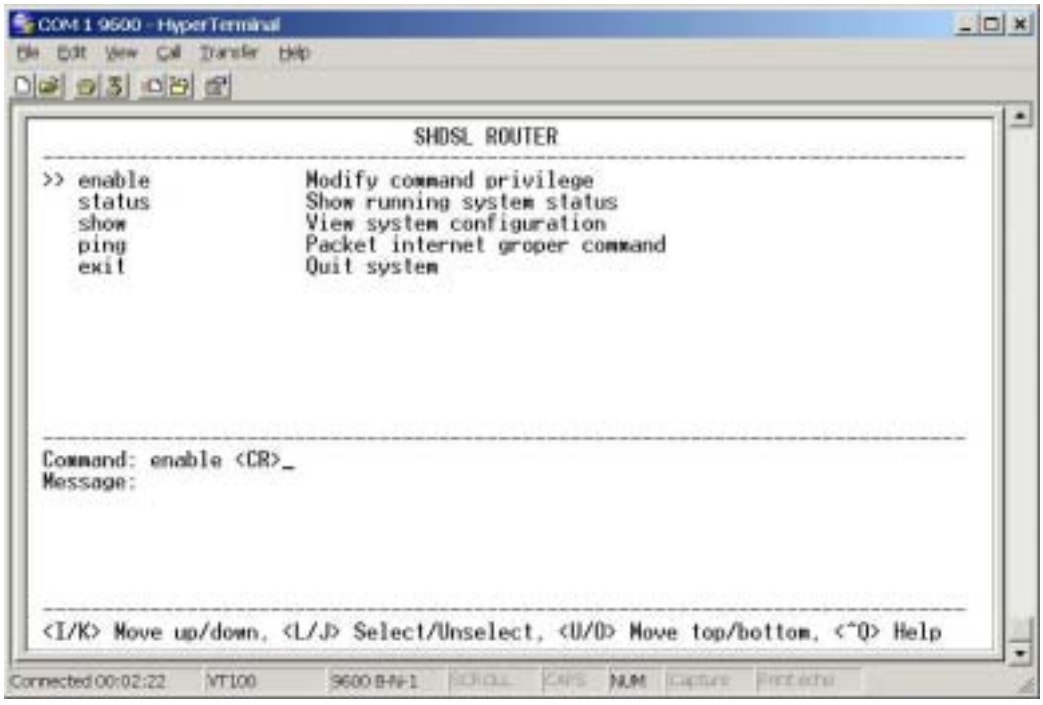
3.4 Operation Interface

For serial console and Telnet management, GRT-101 implements two operational interfaces: command line interface (CLI) and menu driven interface. The CLI mode provides users a simple interface, which is better for working with script file. The menu driven interface is a user-friendly interface to general operations. The command syntax for CLI is the same as that of the menu driven interface. The only difference is that the menu driven interface shows you all of available commands for you to select. You don't need to remember the command syntax and save your time on typing the whole command line.

The following figure gives you an example of the menu driven interface. In the menu, you scroll up/down by pressing key I / K, select one command by key L, and go back to a higher level of menu by key J. For example, to show the system information, just logon to GRT-101, move down the cursor by pressing key K twice and select "show" command by key L, you shall see a submenu and select "system" command in this submenu, then the system will show you the general information.

In this chapter, all configuration procedures are explained by command line examples with necessary parameters. When operating in the menu driven interface, just select the corresponding command items from the menu hierarchy to configure the same setting.

Note: GRT-101 invokes menu driven interface when first time logon with default user profile "**admin**". Both interfaces



have on-line help information. To get on-line help, type "**?**" for CLI mode or press CTRL+Q for menu driven interface.

3.4.1 Multi-level password protection

When you login via serial console or Telnet, GRT-101 defaults to a program execution (read-only) privileges to you. To change the configuration and write changes to nonvolatile RAM (NVRAM), you must work in **enable** mode. Follow the steps below to invoke the **enable** mode:

```
admin> enable
Supervisor password: ****
```

Note: The supervisor password is the same as that for web management interface. If you have not change password setting for the web interface of GRT-101, enter "**root**" to enter GRT-101. For more security issues for remote management interfaces such as Telnet and web interface, see section 3.11 Management Security.

You are now in enable mode. The system prompt appears:

```
admin#
```

Follow the steps below to change the user interface:
To select menu driven interface for user profile 1 (default user profile), enter:

```
admin# admin user modify 1 attrib menu
```

The following command select CLI mode for user profile 1:

```
admin# admin user modify 1 attrib command
```

To save your changes enter:

```
admin# write
```

To enable your changes, reboot the system:

```
admin# reboot
```

For the menu interface, there is a method to enable CLI mode temporarily for script input. By pressing CTRL+U simultaneously, you can see the CLI system prompt in the command line window:

```
Command Line Window...
admin#
```

Press CTRL+U again in the command line window to back to the menu driven interface.

Note: See section 3.10 User Profile for more information on how to add, delete, modify, and list user profile.

3.5 Connection Mode

GRT-101 supports two connection modes: bridging and routing. Currently, it comes pre-configured with routing mode. Note that, routing mode and bridging mode cannot be used simultaneously.
To let GRT-101 operate in bridging mode, type:

```
admin# setup mode bridge
```

To save your changes enter:

```
admin# write
```

To enable your changes, reboot the system:

```
admin# reboot
```

To set GRT-101 operating in routing mode, enter:

```
admin# setup mode route
```

To save your changes enter:

```
admin# write
```

To enable your changes, reboot the system:

```
admin# reboot
```

3.6 Bridging Mode

Note: This section is for bridging mode operation only.

When GRT-101 operates in bridging mode, it behaves like a wire connecting a local PC directly to a service provider's network. Bridge data is encapsulated using the RFC1483 protocol to enable data transport. GRT-101 currently supports IEEE 802.1D transparent learning bridge.

3.6.1 Bridge management

You can manage GRT-101 using Telnet either from LAN interface or from Wide Area Network (WAN) interface. The following procedure shows how to

set up GRT-101 for bridging management with IP = 192.168.0.1, subnet mask = 255.255.255.0, and gateway IP = 192.168.0.254:

```
admin# setup lan 1 address 192.168.0.1 255.255.255.0
admin# setup bridge gateway 192.168.0.254
```

The IP address should be an IP address on the same network as that of the "far-end" station. The gateway IP address should be the IP address of the far-end station that is used to route the LAN packets.
To save your changes enter:

```
admin# write
```

To enable your changes, reboot the system:

```
admin# reboot
```

Note: The IP address that is assigned to GRT-101, must be an IP address that is on the same network segment (subnet) that is being bridged. Assigning IP addresses in this fashion enables access via Telnet/web to GRT-101 for management functions. See section 3.11 Management Security for more information on security issues.

3.6.2 Static bridge table

This GRT-101 supports a transparent learning bridge, which will establish the bridge table automatically from the incoming data. Therefore, it is unnecessary to setup the static bridge table manually. In case you need to arrange the static bridge table, see the description below.
The following commands show how to setup the static bridge table by "add" command.

```
admin# setup bridge static add lan_port forward
admin# setup bridge static add wan1_port filter
admin# setup bridge static add mac 00:30:4f:00:00:01
```

Note: You must perform the above procedure in the sequence as shown, i.e., port attributes first and MAC finally.

To list the content of the table, use the "list" command:

```
admin# setup bridge static list
Static Bridging Parameters
  1. MAC Address : 00:30:4f:00:00:01
     <Interface Operation>
     LAN 1(Forward)      WAN 1( Filter)      WAN 2( Filter)      WAN 3( Filter)
```

WAN 4(Filter) WAN 5(Filter) WAN 6(Filter) WAN 7(Filter)
WAN 8(Filter)

To modify the first entry in the table, use the "modify" command:

```
admin# setup bridge static modify 1 mac 00:30:4f:00:00:01
admin# setup bridge static modify 1 lan_port filter
admin# setup bridge static modify 1 wan1_port forward
```

To delete the first entry of the table, use the "delete" command:

```
admin# setup bridge static delete 1
```

To save your changes, enter:

```
admin# write
```

3.7 Routing Mode

Note: This section is for routing mode operation only.

Routing is often confused with bridging, which performs a similar function. The principal difference is that bridging occurs at a lower level (MAC layer) whereas routing occurs at a higher level, e.g., IP layer. And because routing occurs at a higher level, it can perform more complex analysis to determine the optimal path for the packet.
GRT-101 supports IP routing, which can be static and/or RIPv1/v2 updating. Also, several applications, such as NAT/PAT, DHCP server, and DNS proxy, etc., are included for LAN management and control.

3.7.1 LAN setting

To setup GRT-101 LAN interface with IP address of 192.168.0.1 and subnet mask of 255.255.255.0, use the following command:

```
admin# setup lan 1 address 192.168.0.1 255.255.255.0
```

To save your changes, enter:

```
admin# write
```

3.7.2 Static routing table

In order to pass data through a network and onto the Internet or WAN, you might need to add the IP addresses of gateways to the static routing table. Follow the instructions below to build a static routing table manually by adding or deleting entries in the table.
For example, to add a route to network address 140.182.1.0 with subnet mask of 255.255.255.0 via gateway at 140.182.2.254:

```
admin# setup route static add 140.182.1.0 255.255.255.0 140.182.2.254
```

To set a default route with gateway of 140.182.2.254, use the below command:

```
admin# setup route static add 0.0.0.0 0.0.0.0 140.182.2.254
```

In general, it is not recommended to add multiple entries with the format of default route (network address 0.0.0.0 with subnet mask of 0.0.0.0). If there are multiple entries with the format of default route in the static routing table, the system will automatically select only one entry to be the default route among these entries with resolvable gateway.

Note: For most WAN protocols, a valid default route with resolvable gateway on WAN side must be set to work properly. However, for PPP connections, GRT-101 will add default route to ISP gateway automatically, and hence it is unnecessary to add a default route manually.

To enable RIP updating with auto summary for routing table, type:

```
admin# setup route rip generic Enable Enable
```

For detailed configuration about RIPv1/RIPv2, please refer to the on-line help message by the following commands:

```
admin# setup route rip lan 1

admin# setup route rip wan 1
```

Note: Each WAN port could be configured independently for RIPv1/RIPv2 updating of routing table.

To show the configuration, use the list command:

```
admin# setup route rip list
```

To save your changes, enter:

```
admin# write
```

3.7.3 NAT/PAT

NAT can be used to share an Internet connection, to reduce the requirement for publicly assigned IP addresses, to expand an existing network without affecting existing IP based account schemes, and to hide an internal network schema from public networks.
It is often used in the situation where only one IP address could be assigned for the network, such as a PPP connection to an local ISP, e.g., when your local ISP uses protocols of "PPPoA" or "PPPoE" over the ATM VC, you get a dynamic public IP at the WAN port from your local ISP. All requests originating from the LAN (private network) have their source IP addresses replaced with the public IP address. Only one IP address is visible from the public network. To setup this GRT-101 working for the above example, enter:

```
admin# setup lan 1 attrib Virtual
```

Also, make sure to delete all entries in the NAT/PAT IP pools by the following commands:

```
admin# setup ip_share nat virtual delete <1~5>

admin# setup ip_share nat global delete <1~5>

admin# setup ip_share nat fixed delete <1~128>

admin# setup ip_share pat clear <1~10>
```

Note: The maximum number of hosts on the LAN (private network) is limited to be of 253 in dynamic NAT.

To save your changes, enter:

```
admin# write
```

In some cases, the number of externally visible IP addresses is greater than one and less than the host number being hidden behind GRT-101. You could configure GRT-101 such that it acts as follows. Each time a request is made from a host on the LAN, which is included in virtual IP pool, e.g., pool 3: 192.168.0.2~192.168.0.25. GRT-101 chooses an external IP address already configured in the corresponding global IP pool 3 (e.g., 69.210.1.2~69.210.1.7, which is assigned from your local ISP) that is currently unused, and then performs the translation. This type of situation is only possible when the number of hosts having concurrent requests to the external network is equal to or less than the number of external IP addresses on GRT-101. To setup

GRT-101 working for the above situation where WAN 1 is used to connect to the corresponding ISP, use the below commands:

```
admin# setup lan 1 attrib Virtual

admin# setup ip_share nat global interface 3 1

admin# setup ip_share nat global range 3 69.210.1.2 6

admin# setup ip_share nat virtual range 3 192.168.0.2 24
```

To show the configuration, use the list command:

```
admin# setup ip_share nat global list

admin# setup ip_share nat virtual list
```

Note: The IP translation only works between global and virtual IP pools with the same range number. Totally there are 5 NAT global and 5 NAT virtual IP pools for this purpose.

To save your changes, enter:

```
admin# write
```

In the above example, it might happen that packets from some hosts will be dropped when the number of hosts having concurrent requests to the external network is greater than the number of external IP addresses. If it is necessary to guarantee that some hosts (e.g., 192.168.0.31~192.168.0.33) can access Internet at any time, you can use the fixed IP address mapping pool with extra external IP addresses 69.210.1.8~69.210.1.10, also given from ISP via WAN 1:

```
admin# setup lan 1 attrib Virtual

admin# setup ip_share nat fixed interface 1 1

admin# setup ip_share nat fixed modify 1 192.168.0.31 69.210.1.8

admin# setup ip_share nat fixed interface 2 1

admin# setup ip_share nat fixed modify 2 192.168.0.32 69.210.1.9

admin# setup ip_share nat fixed interface 3 1

admin# setup ip_share nat fixed modify 3 192.168.0.33 69.210.1.10
```

To show the configuration, use the list command:

```
admin# setup ip_share nat fixed list
```

Note: The maximum number of entries in the NAT fixed IP address mapping pool is 128.

To save your changes, enter:

```
admin# write
```

Another function provided by this GRT-101 NAT/PAT is the virtual server mapping. Specific ports on the WAN interface (e.g., WAN 1) are re-mapped to services inside the LAN. As only 69.210.1.8 (e.g., assigned to WAN 1 from ISP) is visible to the Internet, but does not actually have any services (other than NAT off course) running on GRT-101, it is said to be a virtual server. For example, requests with TCP made to 69.210.1.8:80 are remapped to the server 1 on 192.168.0.2:80, other requests with UDP made to 69.210.1.8:25 are remapped to server 2 on 192.168.0.3:25. To set GRT-101 for the above NAT function, use:

```
admin# setup lan 1 attrib Virtual

admin# setup ip_share pat modify 1 interface 1

admin# setup ip_share pat modify 1 port 80

admin# setup ip_share pat modify 1 server 192.168.0.2 80

admin# setup ip_share pat modify 1 protocol TCP

admin# setup ip_share pat modify 1 name httpd

admin# setup ip_share pat modify 2 interface 1

admin# setup ip_share pat modify 2 port 25

admin# setup ip_share pat modify 2 server 192.168.0.3 25

admin# setup ip_share pat modify 2 protocol UDP

admin# setup ip_share pat modify 2 name mail
```

To show the configuration, use the list command:

```
admin# setup ip_share pat list
```

Note: The maximum number of service mapping supported by GRT-101 is 10.

To save your changes, enter:

```
admin# write
```

3.7.4 DHCP server

The DHCP server application automatically assigns IP addresses to DHCP clients. Follow the steps below to enable the DHCP applications. The example sets a DHCP server, which could service 50 DHCP clients. The available IP addresses for DHCP clients are located from 192.168.0.2 to 192.168.0.51. In this example, the LAN environment is configured with gateway of 192.168.0.1 and subnet mask of 255.255.255.0. The IP address of 168.95.1.1 is set as a DNS server.

```
admin# setup dhcp generic active Enable

admin# setup dhcp generic ip_range 192.168.0.2 50

admin# setup dhcp generic gateway 192.168.0.1

admin# setup dhcp generic netmask 255.255.255.0

admin# setup dhcp generic name_server1 168.95.1.1
```

In most applications, the value of gateway IP address is the same as the LAN IP address of GRT-101. The value of name server IP address should point towards a valid host that provides DNS lookup service. These parameters should be configured correctly, or computers on the LAN may not access Internet.

Note: If the DNS proxy has been configured properly, the "**name_server1**" field in the above DHCP configuration should be set with the LAN IP address of GRT-101.

To save your changes, type:

```
admin# write
```

3.7.5 DNS proxy

DNS is the naming system for IP based networks and the naming service that is used to locate computers on the Internet. A DNS proxy receives DNS request from computers on the LAN, translates them into the encoding on DNS protocol, and forwards to the real DNS server. To enable the DNS proxy, please correctly set up the DNS proxy so that it can point towards real DNS servers on the Internet. The following example shows you how to setup the IP addresses of real DNS servers:

```
admin# setup dns_proxy 168.95.1.1 168.95.192.1 140.92.61.55
```

Note: For PPP connections, GRT-101 will get DNS server IPs from ISP and assign them into DNS proxy automatically if they have been pre-configured by the local ISP.

The maximum number of DNS servers is limited to 3. To save your changes, enter:

```
admin# write
```

3.8 WAN and ATM Virtual Connection

GRT-101 has two types of WAN ports: physical WAN port (SHDSL) and logical WAN ports (WAN 1~8). The physical WAN port connects GRT-101 to the WAN. The logical WAN port or ports allow you to create virtual WAN connections for plural destinations. When configuring the physical WAN port, you can change the SHDSL physical layer protocol setting. To configure logical WAN ports, you must provision ATM virtual connections for each logical connection. The instructions for each are shown below.

3.8.1 SHDSL operation

There are two SHDSL operation modes: STU-R and STU-C. GRT-101 supports both operation modes and automatically trains up to the ideal line speed. This enables the maximum operative rate as determined by the central office SHDSL equipment, or you could configure the connection rate directly.

Note: Optimal line rates are dependent upon the central office equipment base and optimal line conditions.

Follow the procedure below to change SHDSL physical layer setting.
To set the SHDSL operation mode to STU-R, enter:

```
admin# setup shdsl mode STU-R
```

To set the SHDSL operation mode to STU-C, enter:

```
admin# setup shdsl mode STU-C
```

Also, GRT-101 allows you to assign the connection rate directly by setting the *N* parameter of "n*64" command:

```
admin# setup shdsl n*64 <0~36>
```

where "0" indicates that the adaptive mode will be used to automatically train up to the ideal line speed. The other valid value of *N* parameter ranges between 3 and 36. Do not set the *N* value to 1 or 2. For example, to configure the SHDSL physical layer data rate to 256kbps, enter:

```
admin# setup shdsl n*64 4
```

For different region, you might need to set up the SHDSL type to be "Annex_A" or "Annex_B" by the following command:

```
admin# setup shdsl type Annex_B
```

Note that, to let your setting take effect, you have to save your changes and reboot the system by enter:

```
admin# write
```

3.8.2 ATM virtual connection

There are two types of ATM connections: (1) virtual paths, identified by virtual path identifiers (VPI); and (2) virtual circuit, identified by the combination of a VPI and a virtual circuit identifier (VCI). Also, there are two encapsulation methods for carrying bridged and routed PDUs in the payload field of ATM adaptation layer (AAL) type 5, which are defined in RFC 1483, multi-protocol encapsulation over AAL 5. The LLC encapsulation method multiplexes multiple protocols on a single ATM virtual circuit. Each protocol is identified in the 802.2 LLC header of the packet. The VC based multiplexing method carries each protocol on a separate ATM virtual circuit. This method is sometimes used in private networks, in which PVC creation is very economical.

Note: Each VC is expressed as WAN *x*, where *x* is a number between 1 and 8. GRT-101 comes pre-configured with one ATM VC (WAN 1 with VPI/VCI = 0/32) already established. The WAN 1 port is ready to send and receive network traffic via IPoA protocol with LLC encapsulation. You may need to modify the pre-configured ATM VC when communicating across your local ISP network.

For bridging mode operation, you should select Ethernet over ATM (RFC 1483

bridged Ethernet) as the ATM protocol. For routing mode operation, GRT-101 supports Ethernet over ATM (RFC 1483 bridged Ethernet), IP over ATM (RFC 1483 routed IP/RFC 1577), PPP over ATM (RFC 2364), and PPP over Ethernet (RFC 2516). The following example enables the ATM VC WAN 3 with protocol of Ethernet over ATM:

```
admin# setup wan 3 protocol Ethernet
```

where the selectable parameters corresponding to the above ATM protocols are "Ethernet", "IPoA", "PPPoA", and "PPPoE". To disable the pre-configured ATM VC WAN 1, enter:

```
admin# setup wan 1 protocol Disable
```

The valid ranges for the VPI is from 0 to 255. For the VCI, it is between 0 and 65535.
The following example set the VPI/VCI = 0/135 for ATM VC WAN 3

```
admin# setup wan 3 vpi_vci 0 135
```

To change the encapsulation from default LLC to VC-Mux for ATM VC WAN 3

```
admin# setup wan 3 encap VC-Mux
```

To review the new configuration you have changed for WAN 3, type:

```
admin# setup wan 3 list
WAN Interface Parameters
 Int.    Link          IP Address/          Netmask VPI/   VCI Encap. QoS PCR
 ---- -------- ---------------------------- --------- ------ --- ----
WAN 1   Disable
WAN 2   Disable
WAN 3   Ethernet    192.168.3.1/   255.255.255.0     0/   135   VC-Mux UBR 2400
WAN 4   Disable
WAN 5   Disable
WAN 6   Disable
WAN 7   Disable
WAN 8   Disable
```

To save the new WAN port configuration, enter:

```
admin# write
```

3.8.3 ATM traffic shaping

The objectives of ATM traffic management are to deliver quality-of-service (QoS) guarantees for the multimedia applications and provide overall optimization of network resources. Currently, GRT-101 supports two kinds of ATM QoS service: constant bit rate (CBR) and unspecified bit rate (UBR). The CBR connection involves a static amount of bandwidth allocated for those applications of video, voice, and circuit emulation. The bandwidth is characterized by the peak cell rate (PCR) in the configuration. The UBR connection allows you to define the PCR too. However, it has the lowest priority and is with no QoS guarantees. The range of the PCR is from 64 to 2400Kbps.
To set the class of the ATM traffic shaping for WAN 3 to CBR with PCR of 512Kbps, enter:

```
admin# setup wan 3 qos class CBR
admin# setup wan 3 qos pcr 512
```

To review the new configuration you have changed for WAN 3, type:

```
admin# setup wan 3 list
WAN Interface Parameters
 Int.    Link          IP Address/          Netmask VPI/   VCI Encap. QoS PCR
 ---- -------- ------------------------------ --------- ------ --- ----
WAN 1   Disable
WAN 2   Disable
WAN 3   Ethernet    192.168.3.1/   255.255.255.0     0/   135   VC-Mux CBR 512
WAN 4   Disable
WAN 5   Disable
WAN 6   Disable
WAN 7   Disable
WAN 8   Disable
```

To save the new WAN port configuration, enter:

```
admin# write
```

3.8.4 WAN IP address

Note: This sub-section is for routing mode operation with protocol of "Ethernet" and/or "IPoA" only. For PPP connections, it is unnecessary to set the WAN port IP address and subnet mask.

To set the WAN 3 with IP address of 192.168.3.3 and subnet mask of 255.255.255.0, follow the following example:

```
admin# setup wan 3 address 192.168.3.3 255.255.255.0
```

To review the new configuration you have configured, type:

```
admin# setup wan 3 list
WAN Interface Parameters
 Int.    Link          IP Address/          Netmask VPI/  VCI Encap. QoS PCR
 ---- -------- ---------------------------- --------- ------ --- ----
WAN 1   Disable
WAN 2   Disable
WAN 3   Ethernet    192.168.3.3/   255.255.255.0    0/   135   VC-Mux CBR 512
WAN 4   Disable
WAN 5   Disable
WAN 6   Disable
WAN 7   Disable
WAN 8   Disable
```

To save the new WAN port configuration, enter:

```
admin# write
```

3.8.5 ISP profile for PPP

Note: This sub-section is for routing mode operation only.

If your local ISP uses protocols of "PPPoA" or "PPPoE" over the ATM VC, you may need to setup the username and password information provided from your local ISP. The maximum length of username and password for ISP setting is limited to 51. The following command configures the ISP profile for WAN 3 with username "pppoa3@isp.com", password "Fuyg47ds", and idle timeout of 10 minutes:

```
admin# setup wan 3 isp pppoa3@isp.com Fuyg47ds 10
```

To review the new configuration you have configured, type:

```
admin# setup wan 3 list
Int.        ISP account username              Idle time
---- -------------------------------- ---------
WAN 1
WAN 2
WAN 3                          pppoa3@isp.com          10
WAN 4
WAN 5
WAN 6
WAN 7
WAN 8
```

Note: The ISP account information would not be shown if the corresponding WAN port is disabled. The account information is provided from your local ISP. Please ask your local ISP if you do not know the username and password.

The "PPPoA" and "PPPoE" protocols are designed based on the concept of "dial-on-demand". Each time a request is made from a host on the LAN, GRT-101 checks the link status of the WAN ports and transfers the packets if the link status is active. When the link status is not active, it performs login procedure with the account information of ISP profiles and then transfers the packets if login successfully. Once the link has been established successfully, GRT-101 continuously monitors the traffic over WAN links. The "PPPoA" or "PPPoE" section will be cut off if there are no packets over the links during the period of idle timeout. The valid value for idle timeout is from 0 to 300 minutes. The idle timeout of "0" means that the session connects always even there is no traffic over the WAN link. To save the new WAN port configuration, enter:

```
admin# write
```

Note: Currently, the section timeout is set to be 10 minutes. Also, WAN 1 has the highest priority to dial if multiple WAN ports are enabled with PPPoA/PPPoE protocols while WAN 8 has the lowest one. In most applications, PPPoA/PPPoE protocols must work with NAT/PAT. Please refer to section 3.7.3 NAT/PAT for details.

3.9 System Status and Performance

Use the "status" command to display GRT-101 activities. To see a list of applications and interfaces that provide status, enter:

```
admin# status ?
```

```
shdsl <CR>              Show SHDSL status
wan <CR>                Show WAN interface status
route <CR>              Show routing table
```

To display specific information, for example, for the SHDSL interface status and performance, enter:

```
admin# status shdsl

<SHDSL Status>
SHDSL mode              :SHDSL CPE Side
Bitrate                 :512kbps
Tx Power                :13.5dBm
Current SNR Margin      :10.8dB
Attenuation             :35.8dB
CRC Error Count         :0

SHDSL Remote Side Status
Current SNR margin      :10dB
Attenuation             :35dB
CRC Error Count         :0
```

These statistics are:

• CRC error count — The cyclic redundancy check error count.

• Attenuation —The difference in decibels (dB) between the power level received at the near end versus the power level transmitted from the far end.

• Signal-to-Noise (SNR) Margin — The SNR margin represents the amount of increased received signal (in decibels) relative to the noise power level that the unit is designed to tolerate without disconnecting from the network.

To display status of WAN ports, enter:

```
admin# status wan
WAN     IP address      /     NetMask          VPI/ VCI    Enc    Protocol   Active
----- --------------- --------------- --- ----- ------ -------- ------
WAN1    192.168.  1.  1/255.255.255.  0     0/    32    LLC        IPoA       Yes
```

To list active route status currently, type:

```
admin# status route
Flag  Destination /      Netmask    /    Gateway         Interface     Portname
---- ---------------------------------------- ------------ ---------
```

```
S          0.0.0.0/          0.0.0.0/  200.0.8.254      200.0.8.1      WAN1
C       200.0.8.0/  255.255.255.0/  directly          200.0.8.1      WAN1
C     192.168.0.0/  255.255.255.0/  directly      192.168.0.218      LAN
C     127.0.0.1/255.255.255.255/  directly          127.0.0.1 Loopback
```

3.10 User Profile

GRT-101 comes pre-configured with user profile 1 already established, that is, user "admin" with password of "admin" and menu driven user interface. The maximum number of user profiles is limited to 5. You can add, delete, modify, or list the user profiles with the commands in the following examples.

To change anyone of the user name and password, you must provide both items together. For example, to change the password only to "76gu94t" for user profile 1 (default user name "admin"), enter:

```
admin# admin user modify 1 profile admin 76gu94t
```

For user profile 1 with password "76gu94t", to change the username to "titan" type:

```
admin# admin user modify 1 profile titan 76gu94t
```

Certainly, you can change both user name and password in one command line. The maximum length of user name and password is limited to 19.

To set the user interface for an existing user profile, e.g., user profile 1, use "modify" and "attrib" commands:

```
admin# admin user modify 1 attrib command
```

The following commands add a new user profile 2 "test" with password "83fdi7s", and set the user interface to menu mode:

```
admin# admin user modify 2 attrib menu
admin# admin user modify 2 profile test 83fdi7s
```

Note: You must perform the above procedure in the sequence as shown.

To show all user profiles with attributes, type:

```
admin# admin user list
Legal access user profile
  No        User  Name        UI Mode
 ---- ----------------- -----------
```

1	titan	Command
2	test	Menu
3	(Empty)	
4	(Empty)	
5	(Empty)	

To delete user profile 2, enter:

```
admin# admin user clear 2
```

To save your changes, enter:

```
admin# write
```

3.11 Management Security

Since you can manage GRT-101 using Telnet and web browser over the network either from LAN interface or from WAN interface, the management security is important that it prevents invalid access to GRT-101 from Internet. There are extra two levels of protection for GRT-101 Telnet and web servers except login password control:

3.11.1 Telnet port number

You can specify the TCP port number of the Telnet server other than the default TCP port number 23 so that Telnet access to default port number cannot reach GRT-101. The example below shows you how to setup the Telnet TCP port number from default 23 to 47:

```
admin# admin security port 47
```

The valid range of the Telnet port number is between 1 and 65534. To show which TCP port number is set to allow access to GRT-101, type

```
admin# admin security list
Configuration generic parameter
    Telnet listening TCP port                : 47
```

To save your changes, enter:

```
admin# write
```

3.11.2 Legal client IP

You could assign the legal client IP addresses such that only Telnet clients and web browsers at the legal client IP addresses can access GRT-101. The following example specifies a legal IP address 192.168.0.6 in the pool.

```
admin# admin security ip_pool modify 1 192.168.0.6
```

The maximum number in the legal IP pool is limited to 10. To show how many legal client IP addresses are configured to allow access to GRT-101, enter:

```
admin# admin security list

Legal client IP address
  No     Legal IP Address
 ---- ------------------
   1              192.168.0.6
   2              (Empty)
   3              (Empty)
   4              (Empty)
   5              (Empty)
   6              (Empty)
   7              (Empty)
   8              (Empty)
   9              (Empty)
  10              (Empty)
```

An empty table means there is not any constraint on the Telnet client and web browser IP addresses. The example below deletes the first IP entry from the legal IP address pool.

```
admin# admin security ip_pool clear 1
```

To save your changes, enter:

```
admin# write
```

Note: GRT-101 comes pre-configured without any constraint on the legal access IP addresses of Telnet clients and web browsers for convenience. However, it is very important to setup management security to prevent invalid access to GRT-101 from Internet.

3.12 SNMP Support

In addition to managing GRT-101 by means of the command-line applications and web browsers, you can manage the unit by using a simple network management protocol (SNMP) management station. GRT-101 can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security. Currently, SNMP (RFC 1157) and SNMPv2c (RFC 1901) agents are implemented. Also, the management information bases (MIBs) supported by GRT-101 include MIB II right now.

3.12.1 SNMP community

The below example adds GRT-101 into a SNMP community "private", with read/write access right for SNMP managers in the same community.

```
admin# admin snmp community 1 edit enable private read_write
```

To show the setting of SNMP communities with access right, type:

```
admin# admin snmp community 1 list
SNMP Community Pool
  No              Community                    Access Right
 ---- ------------------------------ ------------------
   1                          private            Read_Write
   2                          (Empty)
   3                          (Empty)
   4                          (Empty)
   5                          (Empty)
```

To disable the SNMP community 1, enter the following command:

```
admin# admin snmp community 1 edit disable private read_write
```

To save your changes, enter:

```
admin# write
```

3.12.2 SNMP trap

GRT-101 can generate alarm conditions to SNMP manager via SNMP traps.

The following example configures trap 1 with SNMPv2c encapsulation. The SNMP manager is located at 192.168.0.254 with community "private".

```
admin# admin snmp trap 1 edit 2 192.168.0.254 private
```

To show the setting of SNMP communities with access right, type:

```
admin# admin snmp trap 1 list
SNMP Trap Host Pool
  No              Trap                          IP Address          Version
 ---- ------------------------------ ------------------ -------
   1                              private          192.168.0.254          2
   2                              (Empty)
   3                              (Empty)
   4                              (Empty)
   5                              (Empty)
```

To disable the SNMP trap 1, enter the following command:

```
admin# admin snmp trap 1 edit disable 192.168.0.254 private
```

To save your changes, enter:

```
admin# write
```

3.13 Backup and Restore Configuration

Remember to backup a copy of your configuration file after you have completed configuration of GRT-101 so you can easily recover it when necessary.

3.13.1 Backup configuration

Use "show script" command to dump the system current configuration in script commands. The following is an example.

```
admin# show script
Showing System Configuration...
setup mode Route
setup shdsl mode STU-R
setup shdsl n*64 0
setup shdsl type Annex_A
```

```
setup shdsl margin 0
setup wan 1 protocol IPoA
setup wan 1 address 192.168.1.1 255.255.255.0
setup wan 1 vpi_vci 0 32
setup wan 1 encap LLC
setup wan 1 qos class UBR
setup wan 1 qos pcr 2400
setup wan 1 isp test test 10
...
admin snmp trap 3 edit Disable 192.168.0.254 private
admin snmp trap 4 edit Disable 192.168.0.254 private
admin snmp trap 5 edit Disable 192.168.0.254 private
admin#
```

After dumping the configuration, use the copy and paste function provided by your terminal access program or Telnet program to save it to a text file. Don't miss any script command line, or you would loss part of the configuration.

Note: With "show script" command, the password is printed with "*" instead of the real password characters for security. Therefore, the backup configuration does not contain the password information. Remember to recover correct password information manually after the backup procedure by a text editor. There is no command that could show the password information. You should save your password in a safe place for any eventuality.

3.13.2 Restore configuration

Before you restore the old configuration back to GRT-101, make sure to clear the whole setting back to the factory defaults first with the following command:

```
admin# setup default
Are you sure? (y/n): y
Set OK!
admin#
```

To restore the configuration, copy the content of the whole configuration file, which was saved according to section 3.13.1 Backup configuration, and paste them into the console CLI via your Telnet program or terminal access program. Watch the system messages to ensure every command was accepted by the system successfully.

Note: The Telnet program is recommended during backup process. If only the serial port could be used, carefully add some delay by adjust the line and/or character delay for your terminal access program so that all command could be accepted by the system without error. Also, the configuration file backup with "show script" command has the

password printed with "*" instead of the real password characters for security. Therefore, remember to recover correct password information manually before the restore procedure.

To save your restored configuration and let it take effect, enter:

```
admin# write
```

and reboot the system.

3.14 Software Upgrade

You check the software version of GRT-101 by the command:

```
admin# show system
General system information
 Model              :08A2
 Software Version   :101029E4
 CPU                :MPC850SR(rev.B)
 RAM                :4MB
 Flash              :2MB
 Chipset            :AD20msp930
 Firmware Version   :3130BE6B
 Hostname           :SOHO
 System Time        :152DAY/18HR/12MIN
```

If GRT-101 is out of date, get the latest version from your service provider by the trivial file transfer protocol (TFTP). The TFTP allows you to transfer new software images to upgrade GRT-101. Refer to section 3.13.1 Backup configuration to backup a copy of your configuration file before upgrading it so you can easily recover the configuration when necessary.
The following example shows you how to get a kernel software image from a TFTP server 192.168.0.200, where the image file name is "kernel.bin":

```
admin# upgrade kernel 192.168.0.200 kernel.bin
TFTP server IP address: 192.168.0.200
Upgrade filename: kernel.bin
  Connecting...
  Download
  Byte Transferred :     624641 bytes
  Complete
Transfer Complete, Replace Now? (y/n): y
Writing flash..................... OK!
```

```
Do you want to reboot? (y/n): y
```

Be sure to write the new image to NVRAM and immediately reboot the device to activate it. When you log back onto GRT-101 after the reboot, then you can use the "show system" command to verify the version of the new firmware that is active, and restore your configuration.

Note: All configurations will be cleared during the upgrading procedure. Make sure that you have a backup configuration file before you start the upgrading procedure. See section 3.13.1 Backup configuration for details.